Computer hacking as a social problem

Brian Alleyne

Department of Sociology,
Goldsmiths, University of London

b.alleyne@gold.ac.uk

Abstract

This chapter introduces the ideas and practices of digital technology enthusiasts who fall under the umbrella of "hackers. "We will discuss how their defining activity has been constructed as a social problem and how that construction has been challenged in different ways. The chapter concludes with several policy suggestions aimed at addressing the more problematic aspects of computer hacking.

Introduction

Hacking is an activity that encompasses computer programming, designing and executing solutions to problems by combining software and hardware, modifying and re-purposing digital media, software and digitally controlled hardware products. Hacking sometimes involves circumventing security systems designed to protect computer networks and digital data stores, activities which some hackers and commentators argue should be referred to as "cracking" in order to distinguish breaking into systems from more generic hacking activity.

The first computers were developed during the second world war, with a computer industry emerging in the 1960s, when we see the first representations of hackers and hacking.

According to Levy's (2010) widely-read account, the term "hack" was first conceived as an engineering accomplishment in hardware, and only later came to take on the meaning of an unorthodox and efficient programming solution to a software problem. In computer science a hack is generally seen as an inelegant but effective solution to a software development problem: hacks are at times necessary, but only in the sense of a necessary evil. By contrast, in the computing cultures that emerged in the late 1960s and that have been spreading globally ever since, a hack had more positive connotations: it came to be widely admired for its efficiency and ingenuity, and in an intriguing semantic reversal, would come to be regarded as itself elegant. In variety of hacking where breaking into secure computer systems is the central activity, the hack is an episode or "exploit," in which the hacker successfully circumvents layers of electronic and sometimes physical security in order to gain access to the innards of computer networks.

Who is a hacker? He/she is a highly skilled technologist, often but not always a software programmer, who explores problems in computing and in domains where computing is used, and seeks to develop solutions to these problems. Pioneering research on hackers defined them as technology enthusiasts who fit a particular social profile - young, often male, and highly skilled with computer technology (Jordan and Taylor 1998; Taylor 1999). The characteristic cultural practice of hackers centres on learning and exercising skills in programming and managing computer systems, and making and modifying computer controlled objects. Defining generic traits of hackers are a desire to acquire new knowledge and skills in their field along with peer recognition, seeking excitement, and a penchant for problem solving; often but not always the hacker is anti-authoritarian. These traits are in some cases combined with a desire for personal enrichment, but in most hackers' accounts of their activities this is either not the case or it is only a small part of the overall identity constructed in the account. Hackers who work on free/libre and open-source software (FOSS

or FLOSS) are active in writing, mostly in online forums, about their world-views and identities (Alleyne 2011). I will throughout the chapter refer to such hackers and their activities as "open hacking." In contrast, hackers who work to penetrate secure systems (whose activities I label "clandestine" hacking), with some notable exceptions (e.g. Assange and Dreyfus, 2011; Mitnick, 2011; Mitnick and Simon, 2005), are less willing to represent their work and politics in public, but their activities have been investigated through interviews and personal narratives written by these hackers themselves (Turgeman-Goldschmidt 2005; Verton 2002). While there are key differences between open and clandestine hackers' accounts, the self-representations of all hackers have in common creativity, individuality, adaptability, and originality as core elements of the hacker identity, elements that were identified in Turkle's pioneering work on online activity (Turkle 1995; Turkle and Papert 1990).

Contrary to what one might think, based on news reports and popular film, there is more to hacking than break-in exploits. Hacker-activism or "hacktivism," which combines hacker techniques and tools with political activism (Jordan and Taylor 2004), has become more significant since the 1990s and unsettles binary oppositions of good/open vs. bad/clandestine hackers. Further complicating efforts aimed at understanding hacking are widely circulated myths built on both fictional and real representations of bright but socially-maladjusted youngsters, shadowy corporations and states, and secret spaces of information espionage. William Gibson's bestselling novel *Neuromancer* (1984) pioneered much of the imagery and terminology used to represent hackers in fiction, film, and computer games: "cyberspace"; a "matrix" of networked computer systems and databases; high-value digital data stores that become the target of criminal activity; and the figure of the hacker (most often portrayed as a young male) whose skill is co-opted by sinister forces. In *Neuromancer* as in Stephenson's *Snow Crash* (2002) and in films such as *War Games* (1983) and *Hackers*

(1995), hackers are portrayed as extreme individualists, social misfits with overdeveloped technical skills and often with underdeveloped interpersonal skills. *Neuromancer* was pivotal in constituting the sub-genre of science fiction literature known as "Cyberpunk" (Cavallaro 2000) in which a dystopian world is ruled by giant corporations that rival nation-states in power and influence, and where there is rampant individualism, creeping social decay, and extremes of wealth and poverty.

Conflict or continuum?

Hacking is a complex field of activity. In order to assess hacking from a social problem perspective, we have to delve further into the open and clandestine aspects of hacking, which can appear as both a social conflict and as lying on a continuum. The pioneering hackers of the late 1960s and early 1970s were committed to sharing and openness (Levy 2010; Raymond 2003), commitments that remain characteristic of some hacking cultures. Against this, the 1980s saw the emergence of a new breed of hacker who operated in a clandestine fashion, whose main aim was to circumvent security systems(for reputation) to do damage to these systems (for personal gain). By the early 1990s the dual contradictory faces of hacking were apparent to most observers. The dichotomy between the open and the clandestine in the world of hacking is also articulated in terms of the interplay of "Black Hats," who are clandestine and often portrayed as criminal, versus "White Hats," who work in both open and clandestine modes, but always (ideally) with the intention of upholding the law in their battles against the Black Hats. Complicating the matter even further is the case of ethical hacking, one form of which involves a hacker seeking to penetrate a secure computer network so as to aid the administrators of that network in strengthening their security measures (Harris et al. 2008).

In presenting a core dichotomy of open versus clandestine hackers as a starting point in thinking about hacking as a social problem, I am not arguing that actual hackers and their practices fit tidily on one or the other side of that dichotomy, rather, I employ the two categories in terms of their utility as ideal types. Such abstractions are useful in that they can help us to step back from both the complex reality of hacking and its representations, in order to examine how and why it is sometimes seen as a social problem. In the remainder of this chapter I will elaborate different aspects of hacking that span the open--clandestine continuum. I will look at hacking as deviance, hacking as cybercrime, free and open source hacker cultures, and politically motivated hacking or hacktivism. I will view these aspects through the lens of social constructionism that involves actors, issues, institutions, and processes that are involved in the creation of social problems.

What is a social problem?

As the concept of social problem is dealt with fully elsewhere in this volume, here I will only detail out how I use the term in analyzing computer hacking. While social problems are constructed, and are sites of contestation, this does not mean that real structural conditions do not furnish the context in which social problems emerge. When one or more groups perceive events, processes, or relationships as troublesome, we have a social problem (Jamrozik 2008; Macionis 2007). Not everyone in the given social setting must agree that the situation in question is problematic, nor will the actors agree on the significance or even the existence of structural conditions that influence the putative social problem. It is because there is disagreement among interested parties on what is a social problem and on whether a phenomenon should be classed as such that social problems are of interest to social scientists. Having become aware that something is seen as a social problem, an important question to ask next is “a problem for whom?” The perspective I take in this chapter is the social

constructivist approach (Holstein and Miller 2003; Spector and Kitsuse 2000), which asks us to consider that what counts as a social problem is not given, obvious, or natural, but is the outcome of ongoing debate and sometimes conflict. Of course real social conditions and relations exist, but these have to be framed through some kind of discourse in order to be transformed into social problems. Furthermore, when we conceive a social problem, we are simultaneously working out if and how we can alleviate or eliminate that problem; in the conclusion of this chapter I will raise several policy directions that have proved useful in addressing the problematic aspects of hacking.

Connor (2013) discusses the stages of the problem policy process. The first step is to conceptualise and define a configuration of people, relationships, events, and behaviours that together constitute the problem; then we have to work out what would provide a solution to the problem. Hacking as a social problem has been fabricated in several stages which we can place into historical periods. First, we have identification of hacking as a distinct activity and of hackers as a distinct kind of person; this identification was constructed in the 1970s and early 1980s. Then we have construction of hacking as a problem that requires surveillance and control, it is at this point that the specialised computer security industry emerges in the 1980s and we see an emergent and growing public awareness of hacking. By the time we get to the 1990s, we see clear lines of contestation between open and clandestine hackers; between all hackers and the computer security industry; and a growing public anxiety about hacking.

Computing fears and hopes

The roots of the fabrication of hacking as a social problem lie ultimately in the complex relations of humans to the technologies they create. The technological progress that is a defining characteristic of modernity raised as many questions as it provided solutions to problems (Berman 1988). While computers and robots have for decades been seen as offering relief from dirty, dangerous, and repetitive work, they have also been viewed with some anxiety with respect to the extent to which they might displace and even control humans. Debates around the costs and risks of technology in general, and information and communication technologies in particular, are the base on which computer hacking is fabricated as a social problem. Computer technology is dual-edged in the general public consciousness: on the one hand it offers great possibilities to expand our mental horizons; on the other, many people feel threatened by the complexity of the technology, and ultimately fear loss of control to that technology. So computers present an existential anxiety for humans and computer hacking is the sharp edge of that general anxiety (Taylor 1998).

Threats, both real and imagined, lie at the core of hacking as a social problem: threats to privacy, to public and private property, and to trust. I will introduce each threat only briefly here as the remainder of the chapter will address each in greater detail. First, we have privacy: we all have information about ourselves that we wish to keep private, much of this in the form of digitised information that helps us to move smoothly through our personal and professional lives. Having your identity "stolen" is a justified fear in a world in which so much of our life is carried out online. Many of the systems on which our collective existence depends are based on heavily computerised and interconnected networked infrastructures that are potential targets for computer hackers. Computer hacking can threaten the security of

both public and private property, ranging from corporate assets to public infrastructure to the funds held in the bank accounts of ordinary people.

Hacking can threaten trust. Our contemporary network society relies on trust: trust in the makers of technology, in technology regulatory bodies, and in any users of these systems following appropriate procedures and guidelines. Some forms of computer hacking undermine this trust in that they cause potential and actual users of these systems to become fearful of becoming victims of a hack, and can cause people who would benefit from ubiquitous information technologies to shy away from making use of these technologies. If people are anxious about being victims of hacking, they often self-impose limits on what they do online and so fail to realize some of the very real benefits of, for example, online social networking, online shopping, or telemedicine.

Hacking as deviance

Some forms of hacking have come to be seen as deviance. Here we must shift our perspective away from the more or less strictly legalistic and law-and-order focus of cybercrime (which we will discuss later) to consider hacking as a form of deviance. We define deviance here as attitudes and behaviours that depart from social and cultural norms. Immediately on stating this definition it must be added that social and cultural norms are always contested, and there is never universal agreement on what should count as deviant; nonetheless, widely agreed norms do exist, and to depart from these take on the label and or role of the deviant (Becker 1997; Curra 2000). Throughout this chapter we will see that many of the practices that fall under the umbrella of computer hacking have at one time or another or in one place or another been viewed as deviant, and that the hackers labelled as deviant have contested that labelling.

In debates around intellectual property in a digital economy we see a particularly clear example of how conflicting perspectives and positions lead to the contested construction of an activity as a form of deviance. For many digital natives (persons born in the 1990s into a world characterized by ubiquitous information and communication technologies - even in the poorest societies), long established ideas of property - the norm - do not apply to digital goods. Having grown up with social media and a sharing economy, digital natives feel entitled to access many forms of digital content without paying. Hacking enters into debates around digital property because a key area of hacking covers the development and sharing of knowledge and skill aimed to circumvent the digital locks that enforce property rights in digital goods. This is a legal problem that is also social in that different social actors are arranged across the debate on intellectual property and how to build a sharing economy (DeVoss and Porter 2006; Lessig 2001; Söderberg 2010). There is potential and actual conflict between, on the one hand, persons who see themselves as sharing digital artefacts, and, on the other, those firms and states that see themselves as acting to protect intellectual property. This scenario is one of the most significant and prevalent consequences to hacking as a social problem.

Free and open source counter culture

The sort of hacking that is concerned with free and open source software production, sharing, and modification is one which at first glance seems little relevant to thinking about computer hacking as a social problem. After all, open source hackers work in the open, and share their code and techniques: so where is the problem in this? In order to explore this question, we must first be clear on what is "free" in free and open source software. Free (Libre) and Open

Source Software (FOSS or FLOSS) is free in two senses: the first sense of which concerns free as in having no price; the second sense concerns free as in free access to the source code describing how the software works. Free and open source software is free in the sense of freedom to examine and change the source code (Berry 2004; Söderberg 2008). Given that what is most often constructed as problematic about hacking involves activities that are clandestine (breaking into secure systems, defacing digital content, stealing information or money, injecting malicious code aimed to sabotage a system), it is important that we are clear that not all hacking activity leads to situations with the potential to be socially problematic, and this is true of many forms of open source hacking. Nonetheless, it is not always easy to separate hacking activities as used by open source hackers from those that are used by clandestine and even criminal hackers. To put it another way, in some cases of open source hacking there is no good reason to frame the activity as a social problem, while in others it is not so easy to determine what would contribute to a social problem and what would not, as when a hacker uses code or techniques developed as open source and freely shared, in order to defeat systems of digital protection for intellectual property, or to carry out a clandestine hack aimed at identity theft.

Clandestine hacking, cybercrime, and the darknet

Clandestine hacking ranges from the mildly anti-establishment to the criminal and even to the, rather more controversially, "terrorist." Clandestine hacking activity is directed largely against the infrastructure of state and corporate computer systems. Given that clandestine hackers are just that – clandestine – it is not nearly as straightforward to locate individuals and groups for interview or observation as it is with open hackers. Due to the methodological barriers that arise in trying to research any socially or legally marginal/deviant activity, what we know about clandestine hackers we know largely through work in which a researcher was able to cultivate a good relationship with one or a few hackers and then snowball to others, or through clandestine hackers' self-accounts (e.g. Turgeman-Goldschmidt 2005; Mitnick 2011), or through mainstream media coverage that is frequently sensationalist. From these sources we may build a picture of the person and practices of the clandestine hacker, but we must remain always mindful of the limited nature of the sample available to writers on this phenomenon.

The activities of clandestine hackers comprise penetrating secure systems, information theft, intelligence gathering, and technical attacks designed to make systems malfunction or fail altogether. For some clandestine hackers, circumventing the layers of security in corporate or government computer networks is an achievement in itself; for others it is the first step in getting information for subsequent trade or in order to gain direct access to electronically stored funds or other valuable data. These latter hackers may be individuals working on their own account, or as employees of criminal organisations. For all clandestine hackers, the "exploit" – a successful circumvention or penetration of a secure target – is the focus of their activity. What research there is on clandestine hacking leads to a further division of clandestine hackers into two camps (though individuals may shift from one camp

to the other over the course of a career or even a specific project): first, those who claim to be motivated by a politics of libertarianism and for whom the computer security industry is the front line of repressive corporations and governments; second we have the clandestine hackers who are in the game for personal gain. Both types of clandestine hacker operate under the radar, in large measure because both tendencies are seen as criminal by law enforcement agencies and the computer industry. Insofar as we have sociologically coherent data on persons who fall under these categories, we are dealing with loners, known in their hacker identities only to a small circle of other hackers (and presumably sometimes, to the agencies that seek to police this kind of hacking). Clandestine hacking at its most extreme presents a range of problems, from cybercrime, to the unregulated darknet, to cyberterrorism.

Cybercrime

Cybercrime covers any criminal activity that is either carried out on a computer network or assisted in its execution by computer technology (Wall 2007; Yar 2006). There is overlap between criminality and social problems but not all social problems are crimes. Because crime is an acute social problem, so too is cybercrime. Cybercrime is often but not always executed with the aid of clandestine hacking tools and techniques, but cybercrime should not be conflated with clandestine hacking, because not all clandestine hacking is cybercrime. Cybercrime ranges from breaking into systems and stealing valuable information, using computer networks to aid efforts to defraud or steal in the offline world; producing, circulating, and consuming illicit or illegal images, as for example child pornography; online harassment and stalking; and defacement or sabotage of online information stores. Moreover, given that it is a variety of criminal activity, cybercrime also includes any act typically carried out on a computer or computer network with the aid of a computer or computer network which is deemed illegal in the jurisdiction in question. While cybercrimes come

under the purview of law and order, there is still scope for debate as to the criminal status of acts defined as cybercrime. This in turn gives scope for the input of criminologists and other social scientists into processes of construction, labelling, and response to cybercrime. As with other social problems, cybercrime is the object of struggles over definition and labelling. Different legal jurisdictions work with different understandings of cybercrime, and detection and prosecution of cybercrime varies from place to place (Martin and Rice 2011). Apart from activities such as child pornography or online fraud, on which there is broad agreement as to their criminal status, some activities that are labelled as cybercrime, such as copying and sharing of copyright content or defacement of websites, are objects of intense contestation as to whether they should be treated as criminal acts (Barassi 2015; Jordan 2015). In one tragic example of conflict over what should count as cybercrime, Aaron Swartz was arrested in 2011, accused of criminal activity for downloading and sharing thousands of academic papers from servers at the Massachusetts Institute of Technology (MacFarquhar 2013); in response many open hackers and human rights activists argued that it was absurd to charge him as a criminal. Swartz, a highly skilled programmer who had become a prominent free software, open data and digital rights campaigner, took his own life while awaiting trial.

The darknet

One of the most problematic aspects of hacking culture is that of the the darknet (sometimes referred to as the darkweb), which is an alternative to the net/world wide wide web as we all know it (Bartlett 2015). The darknet is layered on and sits alongside the existing internet, employing a vast array of hidden websites and secret access protocols. In order to gain access to the darknet, you have to go through special sites accessible only via anonymous access points. The darknet is a globally dispersed collection of computer servers, users, technicians, content producers, and whole businesses. While it relies on the same technologies as the

conventional internet, the darknet has different systems of regulation, and relies heavily on peer to peer systems of control because top-down management structures would make it vulnerable to surveillance and penetration by security agencies. The darknet is anarchic, but not chaotic. There are norms on the darknet. Many hacker activists see it as perhaps the greatest effort so far to build a structured system of human relations designed on decentralised (even anarchist) political principles. To its critics, the darknet is a criminal network; to many hackers and activists, the darknet is a self-organised network that is an alternative to an internet that is dominated by private corporations and states that are either neoliberal, authoritarian, or both. Whichever of these views one accepts, the darknet does exist, and there are legitimate concerns regarding trade in dangerous drugs, weapons, and money laundering that take place there. At the same time, there are sound political reasons why many people take advantage of the anonymity offered by the darknet, such as fear of repression for holding divergent political views. The darknet is a response to real problems of freedom and privacy, and it also is also a space in which criminal activity can evade detection and law enforcement.

Profit or pleasure?

So that we do not conflate distinct motives in clandestine hacking (cracking), it is necessary to differentiate those hacking activities whose primary aim is to realise financial gain through illegitimate means, from those whose primary purpose is the technical achievement itself. Of course these two aims can and do overlap but for analytical purposes we should keep them distinct, because they present two distinct kinds of problem. Let us explore this through the example of game modification, or "modding."

Modding a computer game entails persons, other than the creators ordevelopers of the game, making changes to the mechanics of game play, changing or adding new levels,

content and rewards, and even entirely new versions of the game (Hong and Chen 2013). The essence of the game modification or "mod" is that it is the result of activity by outside parties, even though the separation of users from developers/creators is not always clear-cut, and user/creator overlap is itself the object of ongoing debate and research. Modding requires access to the code and digital assets of the game. This access may be had by means of the source code of the game and/or by hooks into the source code, and to the source files of digital assets - images, sound and 3d models. The knowledge and skills of reading and writing code that lie at the core of hacking practice are the same as those required to execute many kinds of mods, because after all, a computer game is fundamentally a software product. A key feature of the contemporary gaming scene is that many game producers provide tools in order to encourage the creation of new content and game play experiences. Whether supported by developers or not, many mods have become as popular as the original games on which they were based. The global game industry is worth tens of billions of dollars annually yet unpaid labour is the norm in game modding. The work of game modding is often a labour of love and it is in this affective character of the work of modding that we can see direct parallels to open hacking. Dyer-Witherford and de Peuter (2009, 23–27) discuss modding as "playbor" – the gaming version of immaterial labour, and review debates around whether game modding should be seen more as an example of the empowerment of players to interact more deeply with and transform their favourite games (the preferred view of game producers), or as a way for game producers to exploit unpaid labour to enhance their products. Whether the modders break copy protection or work with open assets and code, they intend their modifications to be used by others, so the sharing is a defining feature of the game modding scene and one that can bring modders into conflict with owners and distributors of games and related digital content.

Whichever way we look at the issue, there is potential and actual conflict leading to social problems. If we take the perspective of corporate owners of intellectual property in games, then any modification not sanctioned by them is illegal, and therefore the culture of modding that has sprung up is organised illegality. Since game modding can involve circumventing systems of intellectual property protection, firms that own such property see modding as a slippery slope leading from tinkering to illegality. By contrast, in the hacking culture of which game modding is a part, many hackers see themselves as creative individuals who are resisting overbearing corporate control of gaming. To further complicate the matter, if digital locks on a game are broken so that its content or code are copied and used in another for-profit product, we have a case of what many people would recognise as theft. Is the problem of modding mainly to do with people into using games in ways that do not respect the intellectual property rights of the game producers? If so, then unauthorised modding and sharing is a social problem that requires intervention to change attitudes and behaviour. If, by contrast, game modding is seen as an activity that is characteristic of a new digital economy in which property is being redefined through technological change and conflict between social actors with opposed interests, then we have another kind of problem: one of large-scale legal and cultural change that must happen in order to match the new technical reality; in this scenario the social problem then leads to a social movement to redefine the very meaning of property in digital goods (Söderberg 2008). And we must not ignore that both conceptions of modding can - and indeed do - exist. We thus have a social problem of a hacking activity - game modding - that spans radical creativity, deviance, and illegality.

Cyberwarfare and Cyberterrorism

Cyberwarfare refers to conflict between states where that conflict is pursued on computer networks (Richards 2014). The target of cyberwarfare is the computer capability of the opponent and it is not difficult to see how hacking would be central to cyberwarfare, but cyberwarfare is outside the social problem focus of this essay. The related area of cyberterrorism is somewhat more relevant here. As an activity terrorism is generally seen by states to refer to activities intended to instill fear or cause actual harm to groups or to entire populations; cyberterrorism is terrorism on or enabled by computer networks (Embar-Seddon 2002; Kenney 2015). Cyberterrorism is arguably the most extreme case of problematic usage of computer technology because of the potential of successful cyberterrorist attack to cause widespread damage and harm. Cyberterrorist methods are not only limited to computer hacking: if a terrorist attack is enabled by computer technology then it would count as cyberterrorism even if hacking is not directly implicated. Key clandestine hacker skills and tools are core elements of cyber terrorist practice, but then so too can be the tools and techniques developed in FLOSS. While there is an emergent legal definition of cybercrime that has some consensus internationally, cyberterrorism is more difficult to define. What distinguishes cyberterrorism from other problematic forms of hacking is in the aims, objectives and effects, more than the tools and techniques employed. And as with cybercrime, what counts as cyberterrorism depends on the legal jurisdiction in which the act and person accused of cyberterrorism is deemed to be under.

A further problematic aspect of cyberterrorism is not so much that a form of terrorism enabled by high technology would be seen by most people as anything other than problematic, as indeed it is, but that *who* gets labelled as a terrorist depends on how a range of political and cultural issues and conflicts are rendered by powerful social actors (Vegh 2005). Moreover, insofar as the Western world is concerned, since 2001 terrorist threats have been frequently constructed as involving forms of militant Islamism; but what counts as

a dangerous form of Islamism is itself enmeshed in debates about ethnic stereotyping, Islamophobia, and threats to "our [Western] way of life." Thinking on cyberterrorism in the Western world is deeply interwoven with a range of debates over radicalisation and indoctrination into forms of nihilistic and violent politics.

Hacking as a subversive counterculture

When we turn to hacking as a subversive activity we are faced with a range of issues that are relevant from a social problem perspective. We will take "subversive" to mean tending to or actually challenging the existing social and political order. From least to most problematic we have Free and Open Source hacking, challenges to intellectual property, and hacktivism. Open source hacking, very rarely, if ever, raises legal issues and is not a social problem in the sense in which we defined the term in the introduction to this chapter. Because open source hacking is mainly concerned with sharing code and cooperation, there is little at first sight that would appear socially problematic. Long before the networked digital age, political activism occupied a continuum that ranged from expressing disapproval of the political opponent to direct and even violent action.

Some FOSS hacks use tools and techniques that were developed for clandestine hacking, or they may employ clandestine tools as part of a wider project which is not itself intended to circumvent any laws. This can be a murky area because the labelling of hacker tools and techniques as open or clandestine is itself an area of debate and conflict. As we discussed earlier, when the aim of hacking is to challenge existing ideas and practices around intellectual property, legal as well as normative issues come to the fore. Established thinking and practice on ownership of intellectual goods - digital entertainment or educational goods for example - have strong state and legal support in most places. Even though many people (especially those born from the 1990s onward - so-called digital natives) do not see digital goods as the same kind of objects with the same structures of ownership as physical goods, the owners of digital content continue to energetically assert their property rights and to lobby for legal protection against those who copy and share copyright content without paying. The very centrality of software to contemporary life means that it is seen by the firms that make,

sell and support it as intellectual property from which they have a right to derive an economic return. This kind of claim to intellectual property in software is rejected by hackers of all types.

Hacktivism: good causes and fighting the power

As with open source software production and sharing, computer-based or digital activism – "hacktivism"- is an aspect of computer hacking about which it is not easy to take a social problem perspective because activism exists on a continuum ranging from the perfectly legal but oppositional through to the unambiguously illegal, with all points in between. Between the two extremes of open and clandestine, we have hacking as activism, where the hackers work in the open or in secret toward the ultimate aim of using hacking skill to achieve political activist aims (Jordan and Taylor 2004). In this case the hacker is using his or her hacking skills towards clearly defined political ends that cannot always be reduced to either clandestine or open hacking. Given the varied political motivations of hackers, we should not expect in all cases to be able to make a tidy distinction between the role/identity of hacker and hacktivist; depending on the circumstances, perspective or project, the same person may shift between both.

Hacktivsm is manifested in various forms: attacks on websites in order to deny access through overloading – Denial of Service attacks; changing the content of websites to fit the aims of the hacktivst in question; using the web to disseminate an alternative viewpoint and to organise protest and actions (Gerbaudo 2012). In order for activism to morph into hacktivism, the activists in question must either be technically skilled or have access to requisite technical capability; they will define their political objectives such that some form of hacking can at the very least promise the possibility of achieving those objectives. Hacktivism for good causes encompasses humanitarian hacking, some kinds of ethical

hacking, indeed any form of hacking which is shaped by a political project which is oriented towards some clearly stated aim of social or cultural change. In humanitarian hacking, the aim to address needs of people made vulnerable through extreme poverty, conflict, or natural disaster (Haywood 2013). Humanitarian hackers build applications and hardware to support relief efforts. Humanitarian hacking is performed in a context with a clear ethical framework, and in and of itself, does not present a social problem, but humanitarian hackers are always enmeshed in already existing social and political contexts.

What can be socially problematic about political hacking is the "collateral damage" to third parties among the general public which can ensue in the wake of a political hacking exploit. The same hacker who works on a humanitarian hacking project might also work on a political project that is potentially or actually problematic because that political project may contravene particular laws or norms. There is an ambiguity to hacktivism: one person's freedom fighter hacktivist may be another person's criminal. The context of action is key to assessing this kind of hacking as a social problem, precisely because political hacking can range from the perfectly normative legal and broadly accepted political opposition to forms of direct action that threaten established institutions and indeed the state itself. So contextual and case-based analysis would be required in order to make any claim that a particular political hacking project to exploit is a social problem.

Let us take the case of Anonymous (Coleman 2015), an activist collective that came to prominence in 2008 with a high profile hack of the Church of Scientology. In 2010 Anonymous was believed to be one of several hacker groups that organised cyber attacks against the online operations of PayPal, Visa, and MasterCard, as a reaction to these three financial institutions cutting off the supply of donations to WikiLeaks, after WikiLeaks made public a huge quantity of classified US State Department memos in 2010. Anonymous justified these actions in terms of what they saw as an overarching right of the global public

to know what the US and other states were doing through the operations of the intelligence agencies. Even though the leaked documents, having been labelled top-secret, were not intended to be seen by the public, WikiLeaks argued that the US and its allies were using their powers to improperly collect and hold information on private citizens, and also that many of the operations carried out by the US and its allies in the sphere of intelligence were immoral and would not stand up to democratic scrutiny. Anonymous put its member's hacking skills to defend what they saw as the just cause being pursued by WikiLeaks. This put Anonymous in direct confrontation with the government of the United States and its allies, who had labelled WikiLeaks a dangerous organisation and who sought the arrest of its founder, Julian Assange.

Policy responses

Responses to computer hacking as a social problem fall under four broad headings: (1) general public education about hacker cultures; (2) socially and ethically-aware training for computer professionals; (3) outreach programmes aimed to foster socially responsible behaviour in hackers; and (4) improved technical capability to mitigate the negative impact of clandestine hacker exploits. With respect to education, the aim should be to better reach both the general public *and* to develop campaigns aimed towards those groups most likely to get involved in the clandestine aspects of computer hacking. As to improved technical capability, this is largely a matter for governments and the computer security industry; key here is having appropriate systems of oversight of those charged with maintaining information security.

In 2013, Edward Snowden, a US computer programmer and analyst who was at the time a contractor to the US National Security Agency, initiated a leak of classified US government documents that had at least as great an impact as did the Wikileaks leak of 2010; the Snowden leak and subsequent revelations gave further insight into the extent of surveillance carried out by the US government around the world, and intensified debates about surveillance and control that had begun in 2010. As of late 2016, Snowden is resident in Russia where he was granted temporary asylum. The USA continues to seek his appearance in a US court. In the aftermath of these mass leaks, there is justified anxiety in liberal democracies over whether there are effective checks and balances on the actions of state and private security agencies. A democratically debated balance must be struck between security services, on the one hand, and individual rights and privacy, on the other. Such a balance will vary from one context to another. Responses to computer hacking as a social problem must have wide popular legitimacy. If they are imposed fromthe top down, they will be less effective than if they result from the widest possible democratic deliberation.

In a global network society information security is a concern of all of us, and it is precisely because there are ongoing debates about what counts as privacy, security and rights in intellectual property in the digital age, that we need to arrive at responses based on evidence and ultimately on democratic deliberation.

False hope? Cyberutopians and techno-anarchists

In the first decade of the globalizing web (the 1990s), commentary and analysis was focused on the liberatory potential of information technologies; the dominant frame was cyberutopian. Cyberutopianism is a set of ideas and practices based on the assumption that information technologies and especially the World Wide Web are not just a positive development in civilization, but goes further to assert that the very expansion and availability of these technologies would lead to a more prosperous and fairer society at the local, national, and global levels (Rheingold 2000). Cyberutopianism tends to be happy with the existing corporate and governmental structures in liberal democratic capitalist societies, and sees these as being enhanced by the web.

Techno-anarchists, as do cyberutopians, see information technologies as heralding improvements in life for all of us, but where they differ from cyber utopians is in their distrust and open hostility towards existing capitalist enterprise and liberal democratic states. Techno-anarchists look and work toward the destruction of capitalism and the supplanting state structures with non-hierarchical networked democratic systems of social and political organization (Frediani and Ziccardi 2013). Techno-anarchists see information technologies as a way to bring about the radical reduction or total destruction of capitalism and its attendant state structures.

Both cyber utopianism and techno anarchism create at least as many problems as they purport to solve. Social practices that may work in a collective on the margins of a large industrialized society may not scale up to become the norm for that society as a whole. Striking the best balance between individual freedom and privacy on the one hand, and the protection of both private and public property, all the while maintaining law and order, is

hugely complex and requires constant monitoring and ongoing debate. Laws governing what people do with computer and communication technologies must seek to balance the rights of the various parties, in a context where the very meaning of property has shifted.

Representing the full range of hacker cultures

The news mediahave a key role to play in fostering a more complete public understanding of hacking as a complex and widespread culture, *some* aspects of which do pose potential and actual social problems. We need informed and balanced reporting on all aspects of hacking, allowing a range of voices and perspectives to be aired. At the same time the news media have a role to play in alerting the public to the problems that some forms of hacking can pose for society. In addition, news media have a role to play in informing the public about how to embrace the positive aspects of hacking while guarding against the negative. Schools, colleges and universities have a vital role to play here. When we turn to the entertainment industry, we confront the most problematic area for making policy interventions. Artistic freedom, while not without limits in a democratic society, does mean that creators of entertainment products must be free to sensationalize if they wish.

We cannot direct entertainment industries to filter representations of hacking culture. But if the news media and education institutions address the points we set out above, then most people will have the knowledge that would allow them to engage critically with fictional accounts of hacking and so see them as what they are - designed to entertain.

Hacking and the knowledge economy

Computer and information studies curricula must make students aware of the social and legal consequences of computer use, and must foster a sense of responsible and ethical use of these technologies. The already existing curricula for non-specialists must be continually developed and delivered alongside all other areas of education and training for computer specialists.

When we turn to consider policy at the level of national and transnational economies and polities, we must acknowledge that production, consumption, and intellectual property have been refigured by the spread of compute technology into every aspect to life (Benkler 2006). We need to think of new social, political, and economic structures that are adequate to a globalized network society. Hackers will be part of that re-thinking about how best to foster a knowledge-based economy which would provide stable and legitimate employment for persons with an interest in the technologies of hacking. What is important is that policy makers accept that established programmes for teaching information technology and computer science in schools and colleges may not only fail to motivate many persons with an interest in hacking, but can also alienate young people with the aptitude and interest to hack code, driving them toward clandestine networks. What needs to be done is to foster policies that promise to channel early interests in hacking culture in directions that are positive for the individual and away from the illicit.

Notwithstanding the best plans and polices to steer people toward positive aspects of hacking, it is certain that some people will opt for the thrill of breaking into networks and cracking systems of intellectual property protection. Moreover, we must accept that, while there are ongoing political and policy processes of identifying, engaging, and regulating hacker cultures, many hackers will circumvent these policy processes. As in so many areas of social policy, problems and conflict are inherent and cannot be designed away. We should

therefore work toward fostering open and democratic debate about the political, ethical and legal spaces of hacking. The socially and legally problematic aspects of hacking we discussed earlier will not go away, so we have to seek to develop a *modus vivendi* that accommodates the full range of hacking.

Conclusion

There is no straightforward equation of hacking with social problems. Good versus Evil offers a compelling storyline, but is inadequate for fully grasping actual practices of hackers as a social problem, especially when we consider that an individual hacker may shift from one end to another of the open-clandestine continuum. Moreover, how particular hacking activities are read in moral or ethical terms (a first step in constructing hacking as a social problem) is as much dependent on the perspective of the person doing the reading as it is on the actual content of the practices under scrutiny; added to this is the problem of accounting for the intentions of the hacker in question.

Hacking is a complex and varied social and cultural phenomenon involving many identities, relationships, and practices. Hacking has open and clandestine aspects, but these two aspects do not map easily into good/legal vs bad/illegal. While a subset of hacking is clearly socially harmful, most hacking activity cannot be easily labelled as deviant or problematic. There is often a subtle continuum of practice or ideology along which hacking can shift from almost universally accepted as creative and fun engagement with information technologies, to the socially problematic. In a world saturated with information technologies, we require a range of policy responses to the problematic aspects of hacking: these involve proper research, responsible and informed news media coverage, enhanced training of computer technologists in social and ethical issues, greater investment in public education about information technology generally, and about hacker cultures of all types. Whatever polices we put in place, we must accept that some people will hack in order to harm others. The criminal aspects of hacking are a contemporary aspect of wider issues of crime and deviance in all societies. Ultimately we must accept that many persons drawn to hacking will

have an anti-authoritarian political outlook and will simply not be open the wider policy responses as outlined above.

Glossary

Hacking: is the making and modifying of software, digital content, and computer controlled hardware. One distinct variant of hacking involves breaking into secure computer networks (see 'cracking', below).

Cybercrime covers a wide range of illicit and illegal activities that are either enabled or assisted by computer technology, often carried out on computer networks.

Cracking is a form of hacking aimed at circumventing the security of an application, computer or network. Cracking uses many tools and techniques developed by hackers, but is distinguished from generic hacking by a focus on infiltration or theft of information.

Hacktivism is activism combined with hacker practice.It is useful to imagine an ideal continuum with a technically oriented hacking at one end, and with a politically motivated activism at the other; actual hacktivist projects will exist at various points on this continuum.

The Computer Security Industry comprises a plethora of private-sector firms and individual consultants, state agencies and non-governmental organisations, as well as transnational agencies. The central concern is with maintaining the security of the world's

computer systems (which includes of course not only computers and other computing devices but the Internet and World Wide Web).

Digital Rights Management (DRM) comprises various hardware and software systems that control access to a digital product. The best known examples are those systems of encryption used to restrict access to digital video, music and e-books.

Darknet: The darknet (sometimes referred to as the darkweb) is the alternative Internet that is not known to most people. It is a globally dispersed collection of computer servers, users, technicians, content producers, and whole businesses, which interoperates with the global World Wide Web, but works along channels that are hidden from the view of everyday users of the Web.

Social engineering: In the context of hacker cultures, this refers to using techniques of deception and persuasion to get people to reveal confidential or sensitive information that can be used to carry out some form of hacking or cracking : a classic case is getting someone voluntarily to reveal their system password, or to hand over a physical or electronic key.

REFERENCES

Alleyne, Brian. 2011. "Challenging Code: A Sociological Reading of the KDE Free Software Project." *Sociology* 45 (3): 496–511.

Assange, Julian, and Suelette Dreyfus. 2011. *Underground*. Editions des Equateurs.

Barassi, Veronica. 2015. *Activism on the Web: Everyday Struggles against Digital Capitalism*. Routledge New Developments in Communication and Society Research 4. New York: Routledge.

Bartlett, Jamie. 2015. *The Dark Net*. Windmill Books.

Becker, Howard Saul. 1997. *Outsiders: Studies in the Sociology of Deviance*. New ed. New York: Free Press.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, Conn: Yale University Press.

Berman, Marshall. 1988. *All That Is Solid Melts into Air: The Experience of Modernity*. New York: Penguin.

Berry, David M. 2004. "The Contestation of Code: A Preliminary Investigation into the Discourse of the Free/libre and Open Source Movements." *Critical Discourse Studies* 1 (1): 65–89.

Cavallaro, Dani. 2000. *Cyberpunk and Cyberculture: Science Fiction and the Work of William Gibson*. Continuum International Publishing Group - Athlone.

Coleman, Gabriella. 2015. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Reprint edition. Verso Books.

Connor, Stuart. 2013. *What's Your Problem? Making Sense of Social Problems and the Policy Process*. Northwich: Critical Publishing.

Curra, John. 2000. *The Relativity of Deviance*. Thousand Oaks, CA: Sage Publications, Inc.

DeVoss, Dànielle Nicole, and James E. Porter. 2006. "Why Napster Matters to Writing: Filesharing as a New Ethic of Digital Delivery." *Computers and Composition* 23 (2): 178–210.

Dyer-Witheford, Nick, and Greig de Peuter. 2009. *Games of Empire: Global Capitalism and Video Games*. University of Minnesota Press.

Embar-Seddon, Ayn. 2002. "Cyberterrorism." *American Behavioral Scientist* 45 (6): 1033–43.

Frediani, Carola, and Giovanni Ziccardi. 2013. *Inside Anonymous: A Journey into the World of Cyberactivism*. Informant.

Gerbaudo, Paolo. 2012. *Tweets and the Streets: Social Media and Contemporary Activism*. Pluto Press.

Gibson, William. 1984. *Neuromancer*. New York: Ace.

Harris, Shon, Allen Harper, Chris Eagle, and Jonathan Ness. 2008. *Gray Hat Hacking, Second Edition: The Ethical Hacker's Handbook*. 2nd ed. McGraw-Hill Osborne.

Haywood, Douglas. 2013. "The Ethic of the Code: An Ethnography of a 'Humanitarian Hacking' Community." *The Journal of Peer Production*, no. 3 (July). http://peerproduction.net/issues/issue-3-free-software-epistemics/peer-reviewed-papers/the-ethic-of-the-code-an-ethnography-of-a-humanitarian-hacking-community/.

Holstein, James A., and Gale Miller, eds. 2003. *Challenges and Choices: Constructionist Perspectives on Social Problems*. Hawthorne, N.Y: AldineTransaction.

Hong, Renyi, and Vivian Hsueh-Hua Chen. 2013. "Becoming an Ideal Co-Creator: Web Materiality and Intensive Laboring Practices in Game Modding." *New Media & Society*, March.

Jamrozik, Adam. 2008. *The Sociology of Social Problems: Theoretical Perspectives and Methods of Intervention*. Cambridge, U.K. ; New York: Cambridge University Press.

Jordan, Tim. 2015. *Information Politics: Liberation and Exploitation in the Digital Society*. Digital Barricades : Interventions in Digital Culture and Politics. London: Pluto Press.
Jordan, Tim, and Paul Taylor. 1998. "A Sociology of Hackers." *Sociological Review* 46 (4): 757–80.
———. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* Routledge.
Kenney, Michael. 2015. "Cyber-Terrorism in a Post-Stuxnet World." *Orbis* 59 (1): 111–28.
Lessig, Lawrence. 2001. *The Future of Ideas : The Fate of the Commons in a Connected World*. 1st ed. New York: Random House.
Levy, Steven. 2010. *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition*. 1st ed. O'Reilly Media.
MacFarquhar, Larissa. 2013. "Requiem for a Dream." *The New Yorker*, March 11. http://www.newyorker.com/magazine/2013/03/11/requiem-for-a-dream.
Macionis, John J. 2007. *Social Problems*. 3 edition. Upper Saddle River, N.J: Pearson.
Martin, Nigel, and John Rice. 2011. "Cybercrime: Understanding and Addressing the Concerns of Stakeholders." *Computers & Security* 30 (8): 803–14.
Mitnick, Kevin. 2011. *Ghost in the Wires: My Adventures As the World's Most Wanted Hacker*. Little Brown & Co (T).
Mitnick, Kevin D., and William L. Simon. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons.
Raymond, Eric S. 2003. *The Art of Unix Programming*. Harlow: Addison-Wesley.
Rheingold, Howard. 2000. *The Virtual Community: Homesteading on the Electronic Frontier*. Rev. ed. Cambridge, Mass. ; London: MIT Press.
Richards, Julian. 2014. *Cyber-War: The Anatomy of the Global Security Threat*. 2014 edition. Palgrave Pivot.
Söderberg, Johan. 2008. *Hacking Capitalism: The Free and Open Source Software Movement*. Routledge Research in Information Technology and Society. London: Routledge.
———. 2010. "Misuser Inventions and the Invention of the Misuser: Hackers, Crackers and Filesharers." *Science as Culture* 19 (2): 151–79.
Spector, Malcolm, and John I. Kitsuse. 2000. *Constructing Social Problems*. New edition edition. New Brunswick, NJ: Transaction Publishers.
Stephenson, Neal. 2002. *Snow Crash*. New Ed. Penguin.
Taylor, Paul A. 1998. "Hackers: Cyberpunks or Microserfs?" *Information, Communication & Society* 1 (4): 401–19. d
———. 1999. *Hackers: Crime in the Digital Sublime*. Routledge. http://portal.acm.org/citation.cfm?id=519449&dl=GUIDE&coll=GUIDE&CFID=81023245&CFTOKEN=92720362.
Turgeman-Goldschmidt, Orly. 2005. "Hacker's Accounts: Hacking as a Social Entertainment." *Soc. Sci. Comput. Rev.* 23 (1): 8–23.
Turkle, Sherry. 1995. *Life on the Screen: Identity in the Age of the Internet*. London: Phoenix.
Turkle, Sherry, and Seymour Papert. 1990. "Epistemological Pluralism: Styles and Voices within the Computer Culture." *Signs: Journal of Women in Culture and Society* 16 (1): 128.
Vegh, Sandor. 2005. "The Media's Portrayal of Hacking, Hackers, and Hacktivism before and after September 11." *First Monday [Online]* 10 (2). http://firstmonday.org/issues/issue10_2/vegh/index.html.
Verton, Dan. 2002. *The Hacker Diaries: Confessions of Teenage Hackers*. McGraw-Hill Professional.
Wall, David. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Crime and Society Series. Cambridge, UK: Polity.

Yar, Majid. 2006. *Cybercrime and Society*. London: SAGE Publications.